PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of

James Ching-Shau YIK et al. Group Art Unit: 2134

Serial No. 09/866,259 Examiner: Roderick Tolentino

Filed: May 25, 2001

For: DATA NETWORK NODE HAVING ENHANCED SECURITY FEATURES

REQUEST FOR RECONSIDERATION

Sir:

Applicant respectfully requests reconsideration of the rejection of claims 1-14 as set forth in the Office Action dated April 10, 2007.

The Examiner has rejected claims 1, 3-7, and 10-14 under 35 U.S.C. 103(a) as being obvious in view of Badger, "Digital Signature Protection of the OSFP Routing Protocol" and in view of U.S. Published Application 2003/0014665 by Anderson *et al.*

One basic function of Layer 2 switching is MAC address learning. MAC address learning is an automated process by which the source MAC address of incoming packets is automatically associated with the physical port on which the packet arrives. For example, address A can be associated in this way with switch port P. As a result of this MAC address learning, a subsequent packet with a destination MAC address of A will be forwarded to port P. The MAC address learning is carried out on each switch separately, since it associates a port on the switch with a MAC address.

Address-port associations can also be relearned. If a later packet arrives over port Q with a source MAC address of A, then the port associated with MAC address A is switched from P to Q. However, this reveals a security flaw in Layer 2 learning. A malicious device could send packets with a source MAC address A from port Q, thereby

changing the port association of MAC address A. From that point forward, a packet with destination MAC address A will be forwarded to port Q rather than to the proper port P. In this way, a rogue device could intercept traffic destined to MAC address A by having such traffic routed through port Q instead of allowing it to be forwarded properly through port P.

The present invention addresses this problem by various means. Certain MAC addresses-port associations can be protected by preventing them from being changed without supervision. Packets that attempt to change a protected address-port association can be trapped or discarded or can alert management software to the anomaly. MAC address learning can be disabled altogether for certain ports if a problem has been detected or is suspected. Forwarding of traffic with an unknown destination to any port for which MAC address learning is disabled can be disabled, so as to prevent malicious snooping. The MAC address learning for a port may be limited to a maximum number of address association changes. Packets arriving on a learning-disabled port and for which the source MAC address is either not recognized at all or is not associated with the port of origin may be discarded or trapped.

In summary, the purpose of the present invention is to restrict Layer 2 MAC address relearning by controlling and protecting port-address associations.

Badger teaches a method unrelated to the methods of the present invention. Badger teaches a method of protecting routing information that is disseminated throughout an entire network, in particular protecting the OSPF routing protocol. Badger accomplishes this by using cryptography and digital signatures by routers which propagate the routing information to other routers. Section 4.3 of Badger is concerned with establishment of routes through the entire network when some routers are not authenticated.

Anderson teaches a method for an Internet host to respond to a Denial of Service attack. The Internet host establishes security authentication from an upstream router from which the DoS attack came. Once security authentication is established, the Internet host transmits squelch filters to the upstream router, the squelch filters being generated by the Internet host based on characteristics of the attack traffic. The upstream

router installs the squelch filter. Thereafter, network traffic matching the characteristics defined by the squelch filter is blocked from transmission to the Internet host.

The differences between the present invention and the combination of Badger and Anderson will be demonstrated with reference to the particular elements of the present claims.

Claim 1 includes the limitation that the switching node includes a switching database having a plurality of switching entries, each of the switching entries specifying an association between a data network node identifier and a communication port. This is a feature not taught by Badger or Anderson. The Examiner has cited Section 4.3 of Badger as teaching this element. As argued in response to the previous Office Action, this passage does not teach a switching database storing associations between network node identifiers and communication ports, and in fact Section 4.3 of Badger makes no mention of a switching database. The Examiner seems to be equating "a plurality of authenticated routers using headers in packets to identify which packets [are] allowed to use authenticated paths" with the switching database storing associations between network node identifiers and communication ports. The Applicant respectfully submits that information in packet headers is not the same as information stored in a database.

Claim 1 also includes the limitation that the switching node includes a controller executing a secure switching database update process, whereby an attempt by a hostile data network node to effect a modification of a protected switching entry is prevented when the protection flag is set. This is a feature not taught by Badger or Anderson. The Examiner has cited paragraph 26 of Anderson as teaching this element. Paragraph 26 of Anderson discusses a filter being installed at a router, and the router then using the filter to filter out traffic destined for a particular downstream router or Internet host. The filter characterizes traffic used in a Denial of Service attack detected by the downstream router or Internet host (see also paragraph 25 of Anderson). The filter merely filters "bad" traffic. This passage makes no mention of an attempt by a hostile node to effect a modification of a protected switching entry, the protected switching entry being an association between a node identifier and a port.

Neither Badger nor Anderson are concerned with preventing unauthorized modification of switching entries which associate ports with node identifiers, as

illustrated by the absence of the elements discussed above. Because the Examiner has not shown where Badger or Anderson, either alone or in combination, teach each and every element of claim 1, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 1.

Claim 3 includes the limitation of a plurality of topology discover disable flags, each being associated with a communications port. The Examiner has not indicated where this element is taught by the cited references.

Claim 3 also includes the limitation of a controller executing a secure data transport network topology update process whereby attempts by a hostile data network node to effect at least one addition of a switching entry specifying a communication port associated with a topology discovery disabled physical communications port are disabled. The Examiner has not indicated where this element is taught by the cited references. Furthermore, although Badger does address network topology by means of a routing protocol, Badger does not teach preventing the addition of a switching entry to a switching database when the switching entry relates to a physical communications port for which topology discovery is disabled.

Because the Examiner has not shown where Badger or Anderson, either alone or in combination, teach each and every element of claim 3, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 3.

Claim 4 includes the limitation of a plurality of topology discover disable flags, each being associated with a communications port. The Examiner has not indicated where this element is taught by the cited references.

Claim 4 also includes the limitation of a global unknown destination flood control flag. The Examiner has not indicated where this element is taught by the cited references.

Claim 4 also includes the limitation of a controller implementing a secure PDU forwarding process whereby a received PDU having a destination data node identifier not stored in the switching database is replicated only to physical communication ports having reset topology discovery disable flags. The Examiner has not indicated where this element is taught by the cited references.

Because the Examiner has not shown where Badger or Anderson, either alone or in combination, teach each and every element of claim 4, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 4.

Claim 5 includes the limitation of a plurality of unknown destination flood control flags, each being associated with a communications port. The Examiner has not indicated where this element is taught by the cited references.

Claim 5 also includes the limitation of a controller implementing a secure PDU forwarding process whereby a received PDU having a destination date node identifier not stored in the switching database is replicated only to physical communications ports having reset unknown destination flood control flags. The Examiner has not indicated where this element is taught by the cited references.

Because the Examiner has not shown where Badger or Anderson, either alone or in combination, teach each and every element of claim 5, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 5.

Claim 6 is directed to a method of securely updating a switching database, and recites several steps as elements of the claim. The Examiner has not indicated where Badger or Anderson teach a method of securely updating a switching database, and has not indicated where the various elements of claim 6 are taught by the cited references.

In particular, claim 6 includes the limitation of modifying the communications port specification of a switching entry corresponding to a source data network node identifier (extracted from data traffic received on a source physical communications port) if a switching entry protection flag associated with the switching entry is reset. As discussed above with reference to claim 1, neither Badger nor Anderson discuss limiting modification of a switching database using flags associated with the switching database entry.

Because the Examiner has not shown where Badger or Anderson, either alone or in combination, teach each and every element of claim 6, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 6.

Claim 7 is directed to a method of securely updating data transport network topology information held in a switching database, and recites several steps as elements of the claim. The Examiner has not indicated where Badger or Anderson teach a method

of securely updating data transport network topology information held in a switching database, and has not indicated where the various elements of claim 7 are taught by the cited references.

Because the Examiner has not shown where Badger or Anderson, either alone or in combination, teach each and every element of claim 7, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 7.

Claim 10 is directed to a method of forwarding data traffic having an unknown destination, and recites several steps as elements of the claim. The Examiner has not indicated where Badger or Anderson teach a method of forwarding data traffic having an unknown destination, and has not indicated where the various elements of claim 10 are taught by the cited references.

In particular, claim 10 includes the limitation of replicating received data traffic to each one of a plurality of physical communications ports if a global unknown destination flood control flag is reset. The Examiner has not indicated where this element is taught by the cited references.

Claim 10 also includes the limitation of replicating received data traffic to each of one of the plurality of physical communications ports except physical communications ports having a topology discovery disable feature set, if the global unknown destination flood control flag is set. The Examiner has not indicated where this element is taught by the cited references.

Because the Examiner has not shown where Badger or Anderson, either alone or in combination, teach each and every element of claim 10, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 10.

Claim 11 is dependent on claim 10 and includes the limitations discussed above. Claim 11 also includes the limitation of suppressing the replications of data traffic to the source communications port. The Examiner cites Section 4.3 of Badger as teaching this element. However this passage is silent as to replicating traffic to a source communication port.

Because the Examiner has not shown where Badger or Anderson, either alone or in combination, teach each and every element of claim 11, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 11.

Claim 12 is dependent on claim 10 and includes the limitations discussed above. Claim 12 also includes the limitation that each physical communications port includes an associated unknown destination flood control bit, and suppressing the replication of data traffic to communications ports having the associated unknown destination flood control bit set. The Examiner cites Section 4.3 of Badger as teaching this element. However this passage is silent as to unknown destination flood control bits.

Because the Examiner has not shown where Badger or Anderson, either alone or in combination, teach each and every element of claim 12, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 12.

Claim 13 is directed to a method of forwarding data traffic having a destination unknown, and recites several steps as elements of the claim. The Examiner has not indicated where Badger or Anderson teach a method of forwarding data traffic having a destination unknown, and has not indicated where the various elements of claim 13 are taught by the cited references.

In particular, claim 13 includes the limitation of replicating received data traffic to each one of a plurality of communications ports if unknown destination flood control flags associated with the physical communications ports are reset. The Examiner has not indicated where this element is taught by the cited references.

Because the Examiner has not shown where Badger or Anderson, either alone or in combination, teach each and every element of claim 13, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 13.

Claim 14 is dependent on claim 13 and includes the limitations discussed above. Claim 14 also includes the limitation of suppressing the replication of data traffic to the source communication port. The Examiner cites Section 4.3 of Badger as teaching this element. However this passage is silent as to replicating traffic to a source communication port.

Because the Examiner has not shown where Badger or Anderson, either alone or in combination, teach each and every element of claim 14, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 14.

The Examiner has rejected claim 2 under 35 U.S.C. 103(a) as being obvious in view of Badger, Anderson, and U.S. Patent 5,996,021 issued to Civanlar.

Claim 2 is dependent on claim 1 and includes the limitations discussed above as not being taught by Badger or Anderson. The Examiner has also not shown where these elements are taught by Civanlar.

Because the Examiner has not shown where Badger, Anderson, or Civanlar, either alone or in combination, teach each and every element of claim 2 including those of claim 1, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claim 2.

The Examiner has rejected claims 8 and 9 under 35 U.S.C. 103(a) as being obvious in view of Badger, Anderson, and U.S. Patent 4,893,340 issued to Lubarsky.

Claims 8 and 9 are dependent on claim 7 and include the limitations discussed above as having their presence in Badger or Anderson demonstrated by the Examiner. The Examiner has also not shown where these elements are taught by Lubarsky.

Furthermore, claims 8 and 9 include the limitations of associating a topology discovery disable flag with either the source communications port (claim 8) or with all physical communications ports of the data switching node (claim 9). The Examiner cites column 24 lines 13-27 of Lubarsky as teaching these elements. However this passage does not teach these limitations. Although the passage includes the word "topology", the passage makes no mention of a topology discovery disable flag, let alone associating such a flag with particular communications ports.

Because the Examiner has not shown where Badger, Anderson, or Lubarsky, either alone or in combination, teach each and every element of claims 8 and 9 including those of claim 7, the Applicant respectfully submits that a *prima facie* case of obviousness has not been established against claims 8 and 9.

In view of the foregoing, it is believed that the claims at present on file are in condition for allowance. Reconsideration and allowance of claims 1-14 are courteously solicited.

Respectfully submitted,

September 10, 2007

Lawrence E. Laubscher, Jr.
Registration No. 28,233
Laubscher & Laubscher, P.C.
1160 Spa Road, Suite 2B
Annapolis, MD 21403
Telephone: (410) 280-6608

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence consisting of 9 pages (including cover)is being transmitted to the U.S. Patent and Trademark Office electronically on **September 10, 2007**.

Marianne G. Smith

Signature